

80

Notice of Allowability

Application No.

10/757,742

Examiner

Ronald Baum

Applicant(s)

SZOR ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 9/26/2007.
2. ☒ The allowed claim(s) is/are 1-6, 10-21 and 24-27.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/23/07

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 1-6, 10-21 and 24-27 are allowed over prior art.
2. This action is in reply to applicant's correspondence of 26 September 2007.
3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
4. As per claims 1, 10, 15, 19 and 25 generally, prior art of record, Arnold et al, U.S. Patent No. 6,981,279 B1, fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 26 September 2007 to office action of 7/6/2007.

Specifically, (as per claim 1, for example) prior art dealing with Intrusion Detection for network servers, and associated real time (i.e., CGI scripts, running/executing code access control services, etc.,) detection/scanning associated with attempted malicious behavior/malware, is generally known to exist per se, (i.e., Web server oriented real time access control integrated approaches, inclusive of associated user/managed response aspects, such as GAA-API: Ryutov, T., et al, 'Integrated access control and intrusion detection for web servers', IEEE Transactions on Parallel and Distributed Systems, Vol.14, No.9, 9/2003, entire document <http://ieeexplore.ieee.org/iel5/71/27643/01233707.pdf?arnumber=1233707>). Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., *detecting malicious behavior* in real time of running/executing code, subsequent *blocking of the malicious behavior* associated with the detected running code, *generating a signature associated with the code*, then subsequently *identifying running code* associated with the signature (i.e., versus just the code used for the signature), then allowing the user to *block execution of the identified code*, whereas

Art Unit: 2136

the blocking of the execution is *overridden if the user is incorrectly evaluating the criteria* associated with *the behavior being malicious* (i.e., versus the code per se being malicious)), *at the time of the invention*; serving to patently distinguish the invention from said prior art;

"1. A computer implemented method for *preventing malicious code from propagating in a computer*, the method comprising the steps of:

a blocking-scanning manager

detecting attempted malicious behavior of running code;

responsive to the detection, the blocking-scanning manager

blocking the attempted malicious behavior;

the blocking-scanning manager

generating a signature to identify

the code that attempted the malicious behavior;

the blocking-scanning manager

detecting code identified by the signature,

wherein *detecting code identified by the signature further comprises*

the blocking-scanning manager

alerting a user of the detection; and

the blocking-scanning manager

allowing the user to choose whether or not

to block the execution of the identified code;

the blocking-scanning manager

overriding the user's choice

responsive to the user

incorrectly choosing to block

non-malicious behavior or

incorrectly choosing not to block

malicious behavior; and

the blocking-scanning manager

blocking the execution of the identified code.”.

5. Dependent claims 2-6, 11-14, 16-18, 20, 21, 24, 26 and 27 are allowable by virtue of their dependencies.


Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11,23,07

Ronald Baum

Patent Examiner

